MULTIMEDIA UNIVERSITY®

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2016/2017

ECE3246 – SECURITY & CRYPTOGRAPHY

(CE, ME)

28 FEBRUARY 2017
9:00am - 11:00am
(2 Hours)

INSTRUCTIONS TO STUDENT

1. This examination paper consists of 6 pages including the cover page with 4 questions only.
2. Attempt **any THREE** out of **FOUR** questions. All questions carry equal marks and the distribution of the marks for each question is given.
3. Please print all your answers in the Answer Booklet provided.

Question 1

a) Describe the following security concepts:

(i) the **security property** known as *non-repudiation*.

(ii) *Kerckhoffs' principle.*

[3+3 marks]

b) Consider the MixColumns operation within a round of Mini-AES, wherein multiplication of two nibbles is to be performed modulo a primitive polynomial $m(x) = x^4+x+1$.

Show how the **multiplication** of 0111 and 1011 can be done modulo $m(x)$.

[6 marks]

c) (i) Discuss how a *block cipher* can be used to construct a *message authentication code (MAC).*

[3 marks]

(ii) Given that two parties A and B wish to engage in communications across a public channel that an adversary Z also has access to. Discuss in some detail (i.e. in terms of what the sender could do, what the recipient should be able to do and what the adversary should not be able to do) the main strategies for A and B to achieve **source authentication** (AUTH) between them.

[5 marks]

Question 2

a) Describe your understanding of **stronger/weaker** adversarial *capability* and **stronger/weaker** adversarial *goal*, and discuss which combinations would make a strong *security model.*

[3+3 marks]

b) Discuss the notion of encryption/decryption *oracles* and why these give the adversary more power; then discuss how this adversary capability **compares** with the adversary's knowledge of how to perform encryption/decryption.

[3+3 marks]

Continued...

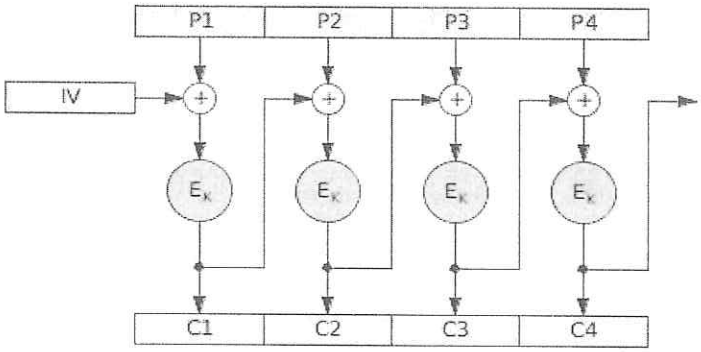

Figure 1 [sourced from Wikipedia]

c) Figure 1 shows a way in which a block cipher E can be used, where the blocks P*1* to P*4* represent the message blocks, and k refers to secret key used to key the encryption E(k).

(i) Discuss *what security* property can be achieved, and *why* it can be achieved, when a block cipher is used in this way. [4 marks]

(ii) Discuss whether the cut-&-splice attack can work, giving your reasons.

[4 marks]

Question 3

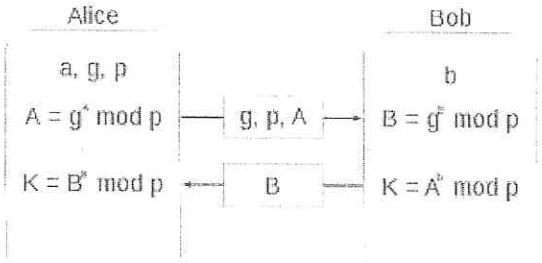

Figure 2 [sourced from Wikipedia]

a) (i) The *discrete log problem* aims to determine x when given $X = g^x \bmod p$ and where the base g and modulus p are also known. Describe the basic idea behind this hard problem, then discuss how this problem relates to the security of the Diffie-Hellman key exchange protocol in Figure 2.

[3+3 marks]

Continued...

b) The RSA public key cipher performs encryption defined as follows

$c = m^e \bmod n$

where c is the ciphertext, m the plaintext, e the public key and n the modulus, and decryption is defined as

$m = c^d \bmod n$.

With some appropriate symbols, notations and/or examples, show why the RSA decryption gets back the plaintext m. [6 marks]

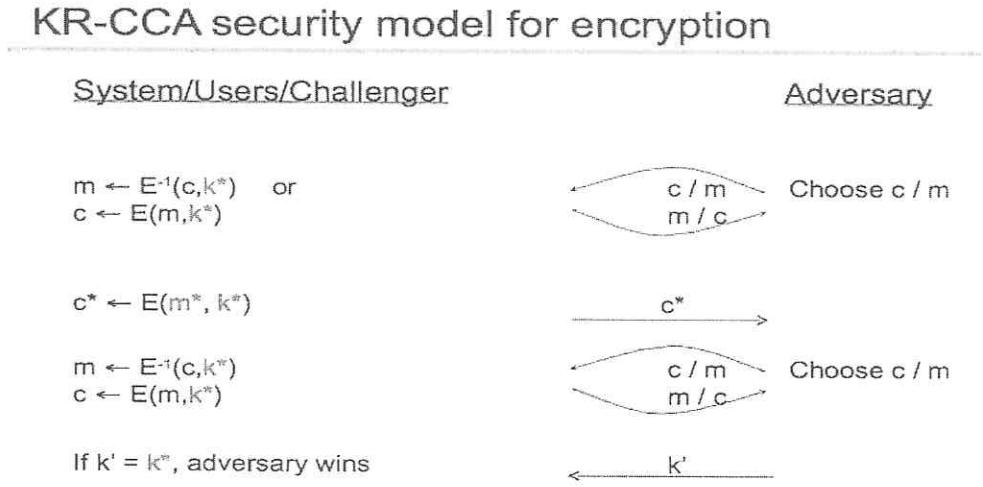

Figure 3

c) Figure 3 shows the key-recovery against chosen-ciphertext attacks (KR-CCA) model.

(i) Using this as a reference, discuss how this model can be changed into the IND-CCA model, where IND denotes indistinguishability. [5 marks]

(ii) Compare between IND-CCA and KR-CCA, explaining which one is stronger as a security model. [3 marks]

Continued...

Question 4

a) (i) Explain your understanding of the difference between defense and resilience. [3 marks]

(ii) Using the Diffie-Hellman key exchange protocol in Figure 2 as an example, describe what you understand by the concept of perfect forward secrecy (PFS) and why it is important for the security of that protocol.

[3 marks]

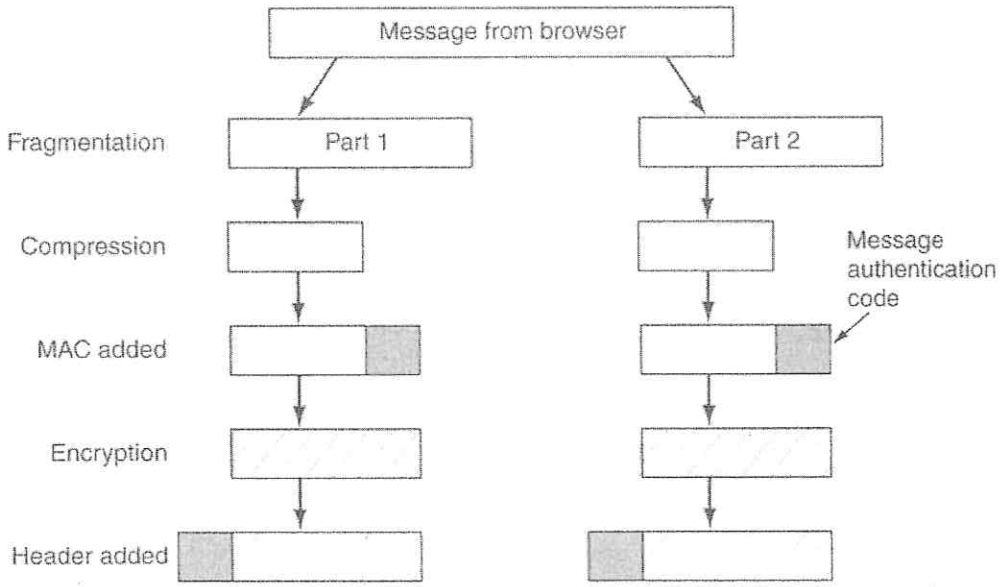

Figure 4

b) (i) Figure 4 shows the process of combining encryption with a message authentication code (MAC). Describe how encryption is combined with MACing for this particular approach. [3 marks]

(ii) Explain what are the security advantages of this approach compared to other ways of combining encryption with MACing.

[3 marks]

Continued...

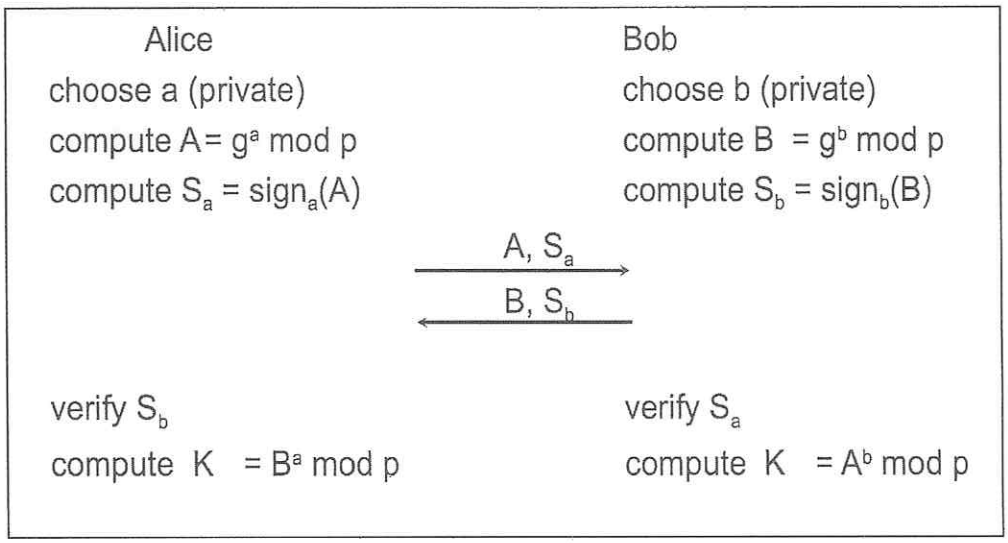

Figure 5

c) Figure 5 shows a variant of the Diffie-Hellman Key Exchange (DHKE) protocol where K is the shared key between Alice and Bob, and $S_A(\ )$ denotes a digital signature signed by Alice. Explain whether/how the following attacks could work:

(i) key-compromise impersonation (KCI) attack. [4 marks]

(ii) known-key security. [4 marks]

End of Paper